

AMENDMENT TO CLAIMS

Please amend the claims as follows:

1-26 (Canceled).

27 (New). A method for communicating with a plurality of devices behind the private side of a NAT, each through a different publicly routable network address, comprising:

issuing a request from a client behind the private side of the NAT to a server on the public side of the NAT for the publicly routable network addresses;

delivering the request from the client to the server through the NAT;

receiving the publicly routable network addresses at the client from the server through NAT;

configuring a router behind the private side of the NAT, named herein a tether router, to associate each of the devices behind the private side of the NAT with at least one of the publicly routable network addresses;

configuring a tunnel through the NAT between the tether router and a router on the public side of the NAT, named herein an anchor router, through which packets can be exchanged between the tether router and the anchor router without being translated by the NAT;

receiving packets at the tether router from the anchor router encapsulated within the tunnel through the NAT addressed to at least one of the publicly routable network addresses; and

forwarding the received packets from the tether router to the device that is associated within the tether router to the at least one publicly routable network address to which the packets are addressed,

whereby communications to the plurality of devices behind the private side of the NAT are effectuated using publicly routable network address.

28. (New) The method of claim 27 wherein the publicly routable network addresses are contiguous.

29. (New) The method of claim 27 where the publicly of routable network addresses are leased.

30. (New) The method of claim 27 wherein the tunnel is configured to automatically reconnect in response to a change in an address associated with one of the components of the tunnel.

31. (New) A method for communicating with a plurality of devices behind the protected side of a firewall, each through a different unprotected network address, comprising:

issuing a request from a client behind the protected side of the firewall to a server on the unprotected side of the firewall for the unprotected network addresses;

delivering the request from the client to the server through the firewall;

receiving the unprotected network addresses at the client from the server through firewall;

configuring a router behind the protected side of the firewall, named herein a tether router, to associate each of the devices behind the protected side of the firewall with at least one of the unprotected network addresses;

configuring a tunnel through the firewall between the tether router and a router on the unprotected side of the firewall, named herein an anchor router, through which packets can be exchanged between the tether router and the anchor router without being translated by the firewall;

receiving packets at the tether router from the anchor router encapsulated within the tunnel through the firewall addressed to at least one of the unprotected network addresses; and

forwarding the received packets from the tether router to the device that is associated within the tether router to the at least one unprotected network address to which the packets are addressed,

whereby communications to the plurality of devices behind the protected side of the firewall are effectuated using unprotected network address.

32. (New) The method of claim 31 wherein the unprotected network addresses are contiguous.

33. (New) The method of claim 31 where the unprotected network addresses are leased.

34. (New) The method of claim 31 wherein the tunnel is configured to automatically reconnect in response to a change in an address associated with one of the components of the tunnel.

35. (New) A system for communicating with a plurality of devices behind the private side of a NAT, each through a different publicly routable network address, comprising:

- a NAT;

- a client configured to:

- issue a request behind the private side of the NAT to a server on the public side of the NAT for the publicly routable network addresses;

- deliver the request from the client to the server through the NAT;

- receive the publicly routable network addresses at the client from the server through NAT;

- a router behind the private side of the NAT, named herein a tether router, configured to:

- associate each of the devices behind the private side of the NAT with at least one of the publicly routable network addresses;

- configure a tunnel through the NAT to a router on the public side of the NAT, named herein an anchor router, through which packets can be exchanged between the tether router and the anchor router without being translated by the NAT;

- receive packets from the anchor router encapsulated within the tunnel through the NAT addressed to at least one of the publicly routable network addresses;

- and

- forward the received packets to the device that is associated to the at least one publicly routable network address to which the packets are addressed,

- whereby the NAT, client, and tether router are configured such that communications to the plurality of devices behind the private side of the NAT are effectuated using publicly routable network address.

36. (New) The system of claim 35 wherein the tether router is configured to automatically reconnect in response to a change in an address associated with one of the components of the tunnel.

37. (New) A system for communicating with a plurality of devices behind the protected side of a firewall, each through a different unprotected network address, comprising:

- a firewall;

- a client configured to:

- issue a request behind the protected side of the firewall to a server on the unprotected side of the firewall for the unprotected network addresses;

- deliver the request from the client to the server through the firewall;

- receive the unprotected network addresses at the client from the server through firewall;

- a router behind the protected side of the firewall, named herein a tether router, configured to:

- associate each of the devices behind the protected side of the firewall with at least one of the unprotected network addresses;

- configure a tunnel through the firewall to a router on the unprotected side of the firewall, named herein an anchor router, through which packets can be exchanged between the tether router and the anchor router without being translated by the firewall;

- receive packets from the anchor router encapsulated within the tunnel through the firewall addressed to at least one of the unprotected network addresses;
- and

- forward the received packets to the device that is associated to the at least one unprotected network address to which the packets are addressed,

- whereby the firewall, client, and tether router are configured such that communications to the plurality of devices behind the protected side of the firewall are effectuated using unprotected network address.

38. (New) The system of claim 37 wherein the tether router is configured to automatically reconnect in response to a change in an address associated with one of the components of the tunnel.